J O I N T C E N T E R
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

Implications of Select New Technologies for Individual Rights and Public Safety*

Amitai Etzioni†

Related Publication 07-15

May 2007

* In preparing this article I greatly benefitted from extensive research assistance by Mackenzie Baris and from comments by Peter Swire, Orin Kerr, and Andrew Volmert. This appeared in the *Harvard Journal of Law & Technology* Volume 15, Number 2 Spring 2002.

† University Professor, The George Washington University.

Executive Summary

In response to the events of 9/11 and to the development of new technologies, the government has enacted new measures to ensure public safety. The article reviews these measures in regard to three communications technologies (cellular phones, the Internet, and high power encryption) and three communications surveillance technologies (Carnivore, the Key Logger System, and Magic Lantern). The first three pose new difficulties for public authorities; the second three help them but might endanger people's rights. Drawing on a communitarian position that there must be a balance between individual rights and the public interest, the article reviews the said measures. Although much of the debate is over whether or not governmental powers are excessive or insufficient, the article argues that the determining factor concerns accountability. If strong enough, powers that might otherwise be excessive might be acceptable. It examines the various ways accountability might take place.

Implications of Select New Technologies for Individual Rights and Public Safety

Amitai Etzioni

Introduction

Are the new measures that have been introduced to protect America from terrorism too extensive, undermining our rights, or are they not extensive enough, leaving the nation vulnerable to future attacks? This article addresses these questions only with regard to those public safety measures, of the more than 150 introduced after 9/11/01,[1] that concern communications surveillance, and among these only the measures relevant to the use of six technologies: cellular phones, the Internet (as a means of communication), high power encryption, Carnivore, the Key Logger System, and Magic Lantern. The article examines the effects of these measures on the use of these technologies and on individual rights and the public interest. The main rights at issue are privacy, anonymity, and due process. The main areas of public interest at issue are public safety and public health, especially prevention of terrorism and response to terrorist attacks once they occur, including bio-terrorism.

The article takes for granted that both individual rights and public safety must be protected, and given that on many occasions advancing one requires some curtailment of the other, the key question is what is the proper balance between these two cardinal values. The concept of balance is found in the Constitution in the Fourth Amendment. The Fourth Amendment refers to people's right not to be subjected to unreasonable search and seizure,[2] hence recognizing a category of searches that are fully compatible with the Constitution: those that are reasonable. Historically, to be considered reasonable, searches have had to serve a compelling public interest, especially public safety or public health.

Much of the debate about the issues at hand in the public arena (by legislatures, opinion makers, and some legal scholars) is conducted in a format familiar in American court rooms: strong advocacy by opposing sides. Thus, one side argues that public safety requires new laws, regulations, and court rulings that would give the government greater surveillance powers, and

1. There were 161 separate provisions in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56 [hereinafter USA Patriot Act].

2. US Const. amend. IV.

warns that major calamities will strike if the government is not accorded these powers.[3] Moreover, the advocates of public safety and health claim that the best way to defend liberty is to provide the government with more authority. Dead people are not free.

The other side does not oppose making concessions to public safety, but puts the onus on the government to prove that such concessions are needed and sets the bar very high for such proof, calling for an approach resembling "strict scrutiny."[4] Although, in the debate since 9/11/01, the civil libertarians' opening position has been to demand a tighter definition of the conditions under which the new technologies can be applied and closer supervision of the expanded governmental powers, ultimately the classical civil libertarian position is that the government needs no additional powers, and moreover cannot be trusted to use any of them legitimately.

From the viewpoint of the paradigm used here, each side is speaking for one side of the needed balance rather than seeking to find the point (or better, zone)[5] at which a carefully crafted balance can be found between protecting the public interest and individual rights.

The quest for balance reflects a new (or responsive) communitarian position developed in the 1990s.[6] Its starting point is that there are two valid claims each society faces: the requirements of the public interest (which most obviously encompasses public safety and health, but also encompasses other elements of the common good, such as the protection of the

---

3. Senator Hatch, during the discussion of USA Patriot on the Senate floor warned:

"I think of the civil liberties of those approximately 6,000 people who lost their lives, and potentially many others if we don't give law enforcement the tools they need to do the job."

CONG. REC. S11023-11024 (daily ed. Oct. 23, 2001) (statement of Sen. Hatch).

4. Nadine Strossen, Remarks at the Communitarian Dialogue on Privacy v. Public Safety (Nov. 26, 2001) (transcript available from the Communitarian Network) [hereinafter Strossen remarks].

5. I refer to a zone because I don't claim that there is a precise point of balance one can identify at which the government tilts clearly in one direction of the other.

6. For further detail on the responsive communitarian position, see the RESPONSIVE COMMUNITARIAN PLATFORM, available at http://www.communitariannetwork.org/platformtext.htm (last modified October 1991); AMITAI ETZIONI, THE NEW GOLDEN RULE (1996) [hereinafter The New Golden Rule]; AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999) [hereinafter The Limits of Privacy. For a critical treatment, see ELIZABETH FRAZER, THE PROBLEMS OF COMMUNITARIAN POLITICS (1999).

environment) and the requirements of liberty (individual rights included).[7] The "turf" does not belong a priori to either claim. It is a gross misconception to argue that public safety measures entail a sacrifice of rights–or vice versa, that respecting individual rights entails sacrifices of the common good. First, in some situations, both can be advanced, such as when restoring law and order to a crime-ridden neighborhood or an anarchic country. Second, when the public interest and rights pose conflicting demands, criteria must be developed as to which should take priority, without assuming a priori that one automatically trumps the other.[8] Judge Richard Posner put the same basic idea in the following way: "I'll call them the public-safety interest and the liberty interest. Neither, in my view, has priority. They are both important."[9]

Such general positions are best examined within an historical context. There is a tendency by societies and polities to tilt in one direction or the other, to lean excessively toward the public interest or liberty. Moreover, corrections to such imbalances tend to lead to over-corrections. For example, the limitations the Church Commission imposed on the FBI in the 1970s, following the abuses of civil rights that occurred during the years J. Edgar Hoover was the director, seem to have excessively curbed the work of the agency in the following decades.[10] The public safety measures enacted since 9/11 have removed many of these restrictions and granted the FBI and other public authorities–such as the Central Intelligence Agency, the National Security Agency, and the military–new powers, arguably titling excessively in the opposite direction. This over-correction has been almost immediately followed by an attempt to correct it (e.g., limiting the conditions under which military tribunals can be used and spelling out procedures not included in their preliminary authorization).[11] At the same time, historical conditions change the point at which we find a proper balance; the 2001 assault on America and the threat of additional attacks constitute such a change.

---

7. See The New Golden Rule, *supra note 6*, chap. 1 and 2.

8. For additional discussion of such criteria, see Amitai Etzioni, *The Spirit of Community* (1993), 177-90; The New Golden Rule, *supra note 6*, at 51-5; and The Limits of Privacy, *supra note 6*, at 10-5.

9. Richard A. Posner, *Security versus Civil Liberties*, THE ATLANTIC MONTHLY, Dec. 2001, at 46.

10. For a short overview of FBI abuses during the 1970s and the responses to them, see CONG. REC. S10992-10994 (daily ed. Oct. 25, 2001) (statement by Sen. Leahy).

11. Katharine Q. Seelye, *Draft Rules for Tribunals Ease Worries, But Not All*, NYTIMES, Dec. 29, 2001, at B7.

The article proceeds by first introducing the relevant aspects of three of the six technologies–cellular telephones, the Internet, and encryption–which have expanded people's free choices, and in this sense their liberties, but have limited the ability of public authorities to engage in the kind of activities they are legally entitled to engage in, especially intercepting communications following court approval. I shall refer to these technologies as *liberalizing technologies*. The article then examines the arguments in favor of and against changing laws and regulations to enable public authorities to cope with, if not overcome, the hurdles posed by the liberalizing technologies in the post-9/11 context.

The article then turns to the three new technologies that help public authorities–Carnivore, the Key Logger System, and Magic Lantern–which have the opposite profile of the first three: they enhance public safety but are feared to curb people's rights. I refer to these as *public protective technologies*. These technologies are then also examined with regard to new laws and regulations and to their effect on the balance between the public interest and individual rights in the post-9/11 context.

Section III of the article calls attention to measures that might help increase public safety while minimizing the threat to individual rights, focusing on the concept of accountability. It should be noted from the outset, the position outlined entails a measure of trust in the government, or at least in some elements of it.

I. NEW LIBERALIZING TECHNOLOGIES

A. New and multiple means of communication

Before the discussion can proceed, it is essential to note that no attempt is being made here to describe fully or to analyze the technologies at issue, but merely to point to features of them relevant to the issues at hand. The year 1980 is used as a baseline. At the time, the most convenient, and by far the most commonly used, way to communicate instantaneously with a person at a different location was through a wired telephone. Cellular phones existed, but they were not yet commercially viable nor were they available in models lightweight enough to put in a pocket.[12] Fax machines had not yet come into wide use.[13] Telegraphs required, as a rule, going

12. JAMES MURRY, WIRELESS NATION (2001) [hereinafter Murry] at 20, 313.

to a post office or Western Union location. Most people had one phone line, even if they had more than one extension. The Internet was still the ARPANET, a government-sponsored network linking mainly universities and research centers.[14] In 1980, all necessary communications surveillance could be carried out easily by attaching simple devices to a suspect's one landline telephone.[15]

In the following two decades, many millions of people acquired several alternative modes of convenient, instantaneous communication, most significantly cellular telephones and e-mail. By July 2000, there were over 100 million cell phone subscribers in the United States.[16] E-mail and Internet usage are similarly pervasive. Nielsen/Net Rating estimated that in July of 2001, 165.2 million people in the United States had home Internet access.[17]

These technological developments greatly limited the ability of public authorities to conduct communications surveillance using traditional methods under old laws (those in effect before the passage of the USA Patriot Act). Attempts were made to apply old laws to new technologies, but they did not fit well. To proceed, it must be noted that there are two types of communications surveillance: public authorities get "pen register" and "trap and trace" orders to obtain only the numbers dialed to or from a specific telephone,[18] or they get full intercept orders to listen to the content of a telephone call.[19] Because the information involved in the first type is

---

13. According to Philip C. W. Sih, though early fax technology was developed in the 19th century, and the US military began using well-developed fax machines during WWII, it was not until the 1970s that the integration of new modem, computer and telephone technologies created the circumstances for a "fax explosion." PHILIP C.W. SIH, FAX POWER (1993), 1-5.

14. PETER SALUS, CASTING THE NET (1995), 82-3.

15. The decision in the Supreme Court case of United States v. New York Tel. Co. Notes that "a pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977). The decision in United States v. Giordano notes that a pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974).

16. Murry, *supra note 12*, at 20, 313.

17. Nielsen/Net Rating for July 2001, available at www.nielsen-netrating.com, (last visited Dec. 6, 2001).

18. 18 USC 3122, 3123.

19. 18 USC 2518.

less sensitive, these orders are much easier to get than the latter.[20] The terms "pen register" and "trap and trace" refer to the devices originally used to carry out the trace orders.[21] Though the technologies they refer to have been replaced, these terms are still commonly used. For the rest of this essay, the term "pen/trap" will be used to designate the type of communications surveillance that involves gathering only the numbers dialed to and from a telephone, or their e-mail equivalent. The term "full" intercept will refer to wiretaps and other means of intercepting the full content of a communication. The term "communications surveillance" will include both pen/trap and full intercept orders.

The law governing full intercepts, contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1969,[22] required that court orders for intercepts specify the location of the communications device to be tapped and establish probable cause that evidence of criminal conduct could be collected by tapping that particular device. Hence, under this law, if a suspect shifted from one phone to another or used multiple phones, the government could not legally tap phones other than the one originally specified without obtaining a separate court order for each.[23] Once criminals were able to obtain multiple cell phones and to "dispose of them as used tissues,"[24] investigations were greatly hindered by the lengthy process of obtaining numerous full intercept authorizations from the courts.[25]

---

20. Smith v. Maryland, 442 U.S. 735 (1979) [hereinafter Smith] established that the use of a pen register to obtain the numbers dialed from a telephone did not constitute a search under the Fourth Amendment, and therefore did not require a warrant. The court held that "it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes."

21. Peter Swire writes: "The term 'pen register' comes from the old style for tracking all of the calls originating from a single telephone. At one point, the surveillance technology for wiretapped phones was based on the fact that rotary clicks would trigger movements of a pen on a piece of paper." Peter Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, BROOKINGS INSTITUTION ANALYSIS PAPER #3, AMERICA'S RESPONSE TO TERRORISM (The Brookings Institution, Washington, DC) Oct. 3, 2001 [hereinafter Swire].

22. Omnibus Crime Control and Safe Streets Act of 1969, Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2521 (1982 & Supp. IV 1986) [hereinafter Title III].

23. 18 U.S.C. 2518 (1)(b)(ii)(1982 & Supp. IV 1986).

24. Rep. Nancy Pelosi, on CNN Novak, Hunt and Shields. Oct. 27, 2001.

25. Victoria Toensing Remarks at the Communitarian Dialogue on Privacy v. Public Safety (Nov. 26, 2001) (transcript available from the Communitarian Network) [hereinafter Toensing remarks].

The rise of Internet-based communications further limited the ability of public authorities to conduct communications surveillance under the old laws. Because Title III did not originally apply to electronic communications, e-mail was often treated as analogous to an older form of communication in the courts.[26] Because e-mails used to largely travel over phone lines, laws governing interception or traces for telephones were extended to govern interception and traces of e-mails as well.[27] However, the language of the old legislation governing pen/trap orders was not clearly applicable to e-mail communications.[28] Though police used pen/trap orders to trace e-mail messages, there was a possibility that a court would rule that e-mail did not fall under pen/trap orders if this was ever challenged in court.[29]

Furthermore, deregulation of the telecommunications industry created additional complications in carrying out pen/trap orders. When the old legislation was enacted, a unified phone network made it easy to identify the source of a call.[30] But e-mail may pass through multiple service providers in different locations throughout the nation on its way from sender to recipient. This means that a service provider might only be able to inform public authorities that a message came from another service provider. In this case, public authorities would have to obtain a new court order from the jurisdiction of that provider to find out where the message came from.[31] Thus, until recently, if a message went through four providers, four court orders in four different jurisdictions would be needed to find out the origin of that message.

---

26. For a discussion of the various analogies applied, see Lt. Col. Joginder Dhillon & Lt. Col. Robert Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*. 56 A.F.L. Rev. 135 (2001) [hereinafter Dhillon] at 149.

27. *Id.*

28. The United States Code defines a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. 3127(3) (1994).

29. Swire, *supra note 21*.

30. *Id.*

31. Field Guide on the New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation, available at: http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf section (last visited January 29, 2002) [hereinafter DOJ Field Guide], 216A.

As with pen/trap orders, the original laws governing full intercept orders did not initially apply to e-mail. However, the Electronic Communications Privacy Act of 1986[32] extended the full intercept laws to apply to electronic communications.[33] E-mail messages differ from phone conversations in important ways that have made the old laws, at best, an imperfect fit.[34] E-mails do not travel over phone lines in discreet units that can just be plucked out. They are broken up into digital packets and travel through the Internet through different routes and mixed together with the packets of the messages of other users.[35] This creates a challenge for law enforcement agents attempting to intercept or trace the e-mail of just one user without violating the privacy of other users.[36]

Problems also occurred when agents received the same search warrants to obtain saved e-mail that they would use in any other physical search.[37] Under old laws, a warrant must be obtained from a judge in the jurisdiction where the search will take place.[38] E-mail, however, is not always stored on a personal computer, but often is stored remotely on the servers of Internet service providers (ISPs). This means that if a suspect, say, in New Jersey had e-mail stored on a

---

32. Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986) [hereinafter, ECPA].

33. The ECPA extended the section of the US Code requiring a court order to intercept oral or wire communications to include electronic communications. 18 USC 2511, as amended by ECPA title I, secs. 101(b), (c)(1), (5), (6), (d), (f)[(1)], 102.

34. For further discussion, see Terrence Berg, *www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law*, 2000 B.Y.U.L. REV. 1305; James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997); Dhillon, *supra note 25* ; Susan Freiwald, *Uncertain Privacy: Communications Attributes Under the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (March 1996); and Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J.L. & TECH. 4 (2001).

35. Christian David Hammel Schultz, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215 (June 2001), 1221-3.

36. Swire *supra note 21*.

37. See 18 U.S.C.A. 2703 (West 2000), which reads: (a) Contents of electronic communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for more than 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

38.18 USC 2703(a).

server located in, say, Silicon Valley, an agent would have to travel across the country to get a warrant to seize the e-mail.[39]

In short, the introduction of both cellular phones and e-mail created new challenges to the ability of public authorities to conduct communications intercepts, even if they were fully authorized by a court–intercepts that had been an important tool of law enforcement. Another technological development has made communications intercepts much more difficult still. Before it is introduced, a brief digression. There is a tendency in parts of the literature on privacy to argue that new technological developments have gravely undermined privacy, if not killed it altogether.[40] In effect, though, the situation in this area is akin to an arms race: as new means of attack are developed, so are new means of defense, although in any given period one side or the other may be the leading beneficiary of new technological developments.

To return to our subject, a major technological development that greatly enhances privacy–and potentially sets back the ability of public authorities to intercept communications–is high power encryption.[41] Although codes have existed for thousands of years,[42] only over the last few have programmers developed encryption systems that use codes 128 bits or longer, which are said to be impossible to crack, even by the National Security Agency (NSA).[43] Moreover, these programs are readily available to private parties at low costs. Stewart Baker, former general counsel for the NSA, said that "encryption is virtually unbreakable by police today, with programs that can be bought for $15."[44] Indeed, these programs are increasingly being routinely

39. DOJ Field Guide, *supra note 30*, section 220.

40. An oft-repeated anecdote that illustrates the point: At the launch of Jini, a wireless device that has the potential to track a user's movements, Sun Microsystems CEO Scott McNealy responded to privacy concerns with the declaration that "You have zero privacy now. Get over it!" For a further discussion, see JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

41. See The Limits of Privacy, *supra note 6*, chap. 3.

42. Deborah Russell and G. T. Gangemi Sr., *Encryption*, *in* BUILDING IN BIG BROTHER, 11 (Lance Hoffman ed.1995).

43. Dorothy E. Denning and William E. Baugh Jr., *Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism* (US Working Group on Organized Crime, National Strategy Information Center, 1997). .

44. Jonathan Krim, *High-tech RBI Tactics Raise Privacy Questions*, The Washington Post, Aug. 14, 2001, at A01 [hereinafter Krim].

built into computers.[45] *This means that the privacy of encrypted messages is much higher than that of any messages historically sent by mail, phone, messenger, carrier pigeon, or other means.* (The same encryption also allows the storing of information in one's computer–personal or corporate–that is much better protected than it ever was under lock and key, or even in safes.)[46]

High power encryption has caused a very major setback for law enforcement.[47] Even when granted a court order, public authorities simply seem unable to implement it.[48]

The consequence of this development has been different from others created by new technologies. In contrast with the situation concerning the multiplication of means of expeditious communication, in which the main factor that constrained public authorities was the obsolescence of laws, in the case of high power encryption, the new technology imposes a barrier all its own. In the other instance, a change of law was sufficient to enable law enforcement to deal with the new challenges posed by the new technologies. Here, the horse was out of the barn by 9/11. It seems impossible to break high power encryption, whatever the courts may authorize.

---

45. STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT–SAVING PRIVACY IN THE DIGITAL AGE (2001) [hereinafter Levy], 310-11.

46. In practice, if it difficult to make the information completely secure, just as it is difficult to completely delete files. For example, if the operating system needs to perform another task while an encryption application is in progress, if will halt the application temporarily and return to it later. Before it halts the program, it writes the encryption application, and its key, to disk as a safety measure. When the application is completed later, many users do not realize that a version of the unencrypted key will remain on the disk until the computer writes it over. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, (1994), 148.

47. FBI Director Louis J. Freeh stated that:

"From 1995-1996, there was a two-fold increase (from 5 to 12) in the number of instances where the FBI's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access."

Hearing on Encryption Before the Senate Committee on the Judiciary, 107th Cong. (2001) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter Freeh statement]. See also, The Limits of Privacy, *supra note 6*, chap. 3.

48. I wrote "seems" because it is not possible to know whether the National Security Agency has found a way to decrypt high-power encryption. However, the great efforts made to gain keys reinforce the view that the NSA has failed in its endeavors to this effect.

B. Legal responses

All in all, these technological developments have provided law-abiding citizens and criminals, Americans and people of other nations, including terrorists, greater freedom to do as they choose, and in this sense they are "liberalizing." At the same time, they have significantly hampered the ability of public authorities to conduct investigations. Some cyberspace enthusiasts welcomed these developments, hoping that cyberspace would be a self-regulating, government-free space.[49] In contrast, public authorities clamored for changing the laws to enable them to act in the new "territory" as they do in the world of old-fashioned, landline telephones.[50] Their pressures led to some modifications in the law before the 2001 attack on America, although the most relevant changes in the law have occurred since. Both the pre- and post-9/11 changes to expand the relevant intercept powers of the authorities are next examined jointly.

1. Roving intercepts

The Electronic Communications Privacy Act of 1986 (ECPA) attempted to update the laws governing communications intercepts to be able to deal with the limitations put on them by the technological developments already discussed by allowing for what are known as "roving wiretaps" in criminal investigations.[51] Roving wiretaps are full intercept orders that apply to a *particular person*, rather than to a *specific communications device*. They allow law enforcement to obtain a court order to intercept that person's communications, without specifying in advance

49. See John Perry Barlow, *Cyberspace Independence Declaration*, issued Feb. 9 1996, available at http://www.eff.org/~barlow/Declaration-Final.html (last visited on January 22, 2002); and Steven Levy, *The Battle of the Clipper Chip*, NY TIMES, 12 June 1994.

50. FBI Director Louis J. Freeh testified that:

"The looming specter of the widespread use of robust, virtually untraceable encryption is one of the most difficult problems confronting law enforcement as the next century approaches. At stake are some of our most valuable and reliable investigative techniques, and the public safety of our citizens. We believe that unless a balanced approach to encryption is adopted that includes a viable key management infrastructure, the ability of law enforcement to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired."

Freeh statement, *supra note 48*.

51. Roving wiretaps were initially introduced in the ECPA, *supra note 31*.

which facilities will be tapped, allowing officers to intercept communications from any phone or computer that the person uses.[52]

The process for obtaining a roving intercept order is more rigorous than that for obtaining the old kind of phone-specific order. The Attorney General's office must approve the application before it is even brought before a judge.[53] Originally, the applicant had to show that the suspect named in the application was changing phones or modems frequently with the *purpose* of thwarting interception,[54] but the Intelligence Authorization Act for Fiscal Year 1999 made it easier to obtain a roving intercept order by replacing the requirement to show "purpose to thwart" with the requirement to show that the suspect is changing phones or modems frequently, and that this practice "could have the effect of thwarting" the investigation.[55] Although roving intercepts have not yet been tested in the Supreme Court, several federal courts have found them constitutional.[56]

Prior to 9/11, the FBI could not gain authorization for using roving intercepts in gathering foreign intelligence or in investigations of terrorism. The USA Patriot Act allows for such roving intercept orders to be granted under the Federal Intelligence Surveillance Act (FISA).[57] FISA was passed in 1978 and provides the guidelines under which the executive branch–not only the president but also the Department of Justice–can obtain authorization to conduct surveillance for foreign intelligence purposes.[58] Agents who wish to conduct surveillance under FISA submit an application first to the Attorney General's office, which must approve all requests (as with

52. 18 U.S.C. 2518 (11)(b) (1994 Supp. IV). The addition of this section was part of the ECPA.

53. 18 USC 2518 (11)(b)(i) (1994 Supp. IV).

54. 18 USC 2518 (11)(b) (1994).

55. Intelligence Authorization Act for Fiscal 1999, Pub. L. No. 105-272, 604, 112 Stat. 2396, 2413 (1998), amending 18 USC 2518 (11)(b)(1994).

56. The most significant case is that of United States v. Petti, 973 F.2d 1441, 1444-45 (9th Cir. 1992) [hereinafter Petti]. For further discussion see also Bryan R. Faller, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO ST. L.J. 2093 (1999).

57. USA Patriot Act, *supra note 1*, section 206 (amending 50 U.S.C. 1805(c)(2)(B)).

58. *Hearing on the Foreign Intelligence Surveillance Act of 1978 Before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary*, 95th Congress, 1t Sess. 13 (1977), reprinted in 1978 ISKCON 3904, 3916.

roving intercepts under ECPA). If the Attorney General finds the application valid, it will be taken to one of seven federally appointed judges, who together make up the Federal Intelligence and Security Court (FISC), for approval. The FISC allows no spectators, keeps most proceedings secret, and hears only the government side of a case.[59]

Initially, FISA was limited to investigations for which foreign intelligence was the sole purpose. USA Patriot modifies FISA so that foreign intelligence need be only a "significant purpose" of an investigation.[60] This change effectively allows FISA to be used as part of "multi-faceted responses to terrorism, which involves foreign intelligence and criminal investigations."[61] Because FISA was originally designed for use in gathering foreign intelligence, communications surveillance conducted under FISA differs from that conducted under Title III criminal investigations in several other ways. Under normal Title III intercepts, anyone whose communications have been intercepted has to be notified after the fact that this happened. Under FISA, people do not have to be notified unless evidence obtained through the interception is to be used against them in court.[62] When FISA evidence is used in court, it is difficult for the defendant to challenge it because he or she cannot see the information agents relied on in making the application for surveillance–this is secret for national security reasons.[63]

2. E-mail surveillance

USA Patriot includes provisions to make it easier for public authorities to trace or seize e-mail messages. It explicitly allows pen/trap orders for computer communications (as already discussed, previous orders had to rely on stretched interpretations of the statutes governing

59. Tom Ricks *A secret US court where one side always seems to win*, CHRISTIAN SCIENCE MONITOR, May 21, 1982.

60. USA Patriot Act, *supra note 1*, section 218 (amending 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B)). See also 147 CONG. REC. S11004.

61. Department of Justice overview of the USA Patriot Act, as entered into the CONG. REC. S 11055 (daily ed. Oct. 25, 2001) [hereinafter DOJ Overview].

62. 50 USC 1806.

63. William Carlsen, *Secretive US court may add to power*, SAN FRANCISCO CHRONICLE, Oct. 6, 2001.

pen/trap for telephones).[64] Traces on telephone lines can usually be fulfilled by the local phone company that issued the line. Tracing e-mail messages, which travel through a variety of routes and may go through multiple carriers, often requires access at different points across the country.[65] As previously explained, following the phone model requires gaining warrants in several locations in order to trace one e-mail message. USA Patriot establishes what are de facto nationwide pen/trap orders,[66] allowing one court order to be used on all the carriers through which messages from an individual pass. When a law enforcement agent discovers that an e-mail message was forwarded to (or from) any carrier, he can serve the original court order to this carrier without getting an additional order from the court in whose jurisdiction the carrier is located. Moreover, because agents cannot know in advance which carriers will be involved, the court order needs to specify only the initial facility at which the pen/trap order will be carried out.

USA Patriot also allows a judge in the district with jurisdiction over the crime under investigation to grant search warrants to seize electronic communications stored outside that judge's jurisdiction.[67] This means that an agent can obtain a warrant from a judge in the jurisdiction where the investigation is taking place to seize e-mail stored by an ISP physically located in another jurisdiction.[68]

3. Dealing with encryption

Previous administrations tried to have "back doors" built into encryption software that would enable public authorities, when needed, to decrypt reportedly unbreakable codes.[69] They

64. USA Patriot Act, *supra note 1*, section 214, 216 (amending 50 U.S.C. 1842, 1843 and 18 U.S.C. 3121, 3123, 3127).

65. *Id.* section 216 A. See also DOJ Field Guide, *supra note 30*, section 216A.

66. The law is worded in a peculiar way, saying that a single order can be used at any carrier's facility, but not explicitly establishing that the order has nationwide scope. *Id.* section 216A

67. *Id.* section 220 (amending 18 USC 2703).

68. *Id.* section 220. See also DOJ Field Guide, *supra note 30*, section 220.

69. See The Limits of Privacy, *supra note 6*, chap. 3; Levy, *supra note 45*, at 226-268.

also attempted to get legislation passed that would require users to deposit a copy of their key with third parties (referred to as "escrow") or public authorities, who would not be able to look at or use the key unless authorized to do so as part of an investigation.[70] A combination of civil liberties groups and high-tech corporations successfully fought off both of these attempts.[71] No attempts to deal with this matter were included in the USA Patriot Act. Further discussion of law enforcement tools to cope with encryption must be deferred until the public protective technologies are discussed.

4. Evaluating the changes in the law

a. General

The adaptations of the laws governing communications surveillance (which includes both pen/trap and full intercept orders) and seizures of stored communications have been subject to both general and detailed debates by the adversarial advocates already mentioned. On the general level, these adaptations were lumped together with numerous other matters including indefinite detention of aliens,[72] allowing the government to listen in on attorney-client conversations,[73] and military tribunals.[74] The nature of the debate on this level is illustrated by statements such as

70. *See, e.g.* Bruce W. McConnell & Edward J. Appal, Draft paper, Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure, available at http://www.epic.org/crypto/key_escrow/white_paper.html (last visited January 29, 2002); and *Hearing on Privacy in a Digital Age: Encryption and Mandatory Access Before the Senate Committee on the Judiciary, Subcommittee on the Constitution, Federalism, and Property Rights*, 105th Cong. (1998) (statement of Robert S. Litt, Principal Associate Deputy Attorney General). For a fuller history of key escrow, see A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. L. FORUM 15.

71. JEDI Callusing, *White House Yields a Bit on Encryption*, NY TIMES, July 8, 1998, D1; Lance J. Hoffman, *Encryption Policy for the Global Information Infrastructure*, statement at the Eleventh International Conference on Information Security, Cape Town South Africa, 9-12 May 1995.

72. USA Patriot Act, *supra note 1*, section 412.

73. AG Order No. 2529-2001, 66 Fed. Reg. (Oct. 31, 2001) (to be codified at 28 CAR pt. 500-501).

74. Military Order of November 13, 2001--Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism.

66 Fed. Reg. 57831-57836 (Nov. 16, 2001).

Senator Patrick Leahy's that some of the measures are "shredding the Constitution"[75] and Morton Halperin's reference to the legislation as "Striking Terror at Civil Liberty."[76] On the other side, Senator Hatch dismissed such misgivings as "hysterical concerns" and said the American people do not want to see Congress "quibble about whether we should provide more rights than the Constitution requires to the criminals and terrorists who are devoted to killing our people."[77] Attorney General John Ashcroft suggested that criticisms of the new powers being requested by the executive branch serve only to "aid terrorists" and "erode our national unity and diminish our resolve."[78]

b. Fourth Amendment issues

There has been some debate in the courts and among legal scholars as to how to apply the Fourth Amendment to the new technologies, as well as to the constitutionality of the new legislation governing these technologies.

Before 1967, the Supreme Court interpreted the Fourth Amendment in a literal way, as applying only to *physical* searches. In the 1928 case of *Olmstead v. United States,* the Court took a strict interpretation of the Fourth Amendment and ruled that telephone wiretaps did not constitute a search unless public authorities entered a home to install the device and that therefore the Fourth Amendment did not apply to them.[79] The justices wrote in their decision that a person is not protected under the Fourth Amendment unless "there has been an official search

---

75. Senator Patrick Leahy, speaking ABC News, *This Week*, (Burwell's Information Services, 18 November 2001): "We don't protect ourselves by bending or even shredding our Constitution. We protect ourselves by upholding our Constitution and demonstrating to the rest of the world we will defend ourselves, but we will do it by also defending our own core values."

76. Morton Halperin, *Less Secure Less Free*, THE AMERICAN PROSPECT, Nov. 19, 2001, at 10.

77. *Hearing on the Department of Justice and Terrorism Before the Senate Committee on the Judiciary*, 107th Cong. (2001) (statement of Sen. Hatch).

78. Attorney General Ashcroft told Congress that tactics of attempting to scare citizens with "phantoms of lost liberty" "only aid terrorists" and "give ammunition to America's enemies."

Hearing on DOJ Oversight: Preserving Our Freedoms While Defending Against Terrorism Before the Senate Committee on the Judiciary, 107th Cong. (2001) (statement of John Ashcroft, Attorney General of the United States).

79. Olmstead v. United States, 277 US 438 (1928).

and seizure of his person, or such a seizure of his papers or his tangible effects, or an actual physical invasion of his house."[80]

In 1967, the Court replaced this interpretation of the Fourth Amendment with the view that it "protects people, not places."[81] In *Katz v. United States*, the Court established a new guideline for determining what falls under the protection of the Fourth Amendment and one that is still in use today–that of a reasonable expectation of privacy.[82] Justice Harlan, in his concurring opinion, set out a two-part test for determining if Fourth Amendment protection applies: the individual must have shown an expectation of privacy, and society must recognize that expectation as reasonable.[83]

Legal scholars have criticized reasonable expectation as the cornerstone of the legal privacy doctrine on a number of grounds that need no reviewing here,[84] but the doctrine is generally still used as a guiding principle. As new technologies emerge, however, the question of what constitutes a reasonable expectation of privacy has to be reexamined in this new context. In the 1996 case of *United States v. Maxwell*, the courts determined that there was a reasonable expectation of privacy for e-mail stored on a server,[85] giving this e-mail, in essence, the same protections given to paper documents stored in an office. In the case of *United States v. Charbonneau*, however, the courts determined that the extent to which one can expect privacy in e-mail communications depends on the context of the situation.[86]

---

80. *Id.* at 466.

81. Katz v. United States, 389 US 347 (1967) [hereinafter Katz] at 351.

82. *Id.* at 351.

83. *Id.* at 361.

84. *See, e.g.* Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384-85 (1974); Richard S. Julie, High-tech Surveillance Tools and the Fourth Amendment: Reasonable Expectation of Privacy in the Technological Age, 37 CRIM. L. REV. 127, 131-33 (2000); Jonathan Todd Laba, If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imagers, Emerging Technologies, and the Fourth Amendment, 84 CALIF. L. REV. 1437, 1470-75 (1996); Scott E. Sundby, "Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 COLUM. L. REV. 1751 (1994); State v. Reeves, 427 So. 2nd at 425 (Dennis, J., dissenting).

85.85. United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

86.United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

Lt. Col. Joginder Dhillon and Lt. Col. Robert Smith argue that because e-mail messages reside on numerous servers between the sending and receiving server, and because on many networks duplicate copies of all e-mails are sent to the system administrator, there may not be a reasonable expectation of privacy for e-mail.[87] This interpretation is backed up by the Supreme Court case *Smith v. Maryland,* in which the Court found that there is no reasonable expectation of privacy for the telephone numbers one dials because those numbers must be conveyed to the phone company.[88] Dhillon and Smith conclude that, at the very least, *Smith v. Maryland* should mean that recording the addressing information of e-mail does not require a full intercept order.[89]

There is some question as to whether or not roving intercepts are in compliance with the Fourth Amendment's *particularity* requirement. The requirement that intercept orders specify the place of the intercept comes from the Fourth Amendment, which states that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[90] Because roving intercepts do not name the location to be tapped, there is some question as to whether or not they are constitutional under the Fourth Amendment.

The argument in favor of their constitutionality is that the particularity of the *person* to be tapped is substituted for the particularity of the *place* to be tapped. In the case of *United States v. Petti*, the Ninth Circuit Court of Appeals upheld the use of roving intercepts, arguing that the purpose of the particularity requirement was to prevent general searches.[91] So long as a warrant or court order provides "sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort" and there is no "reasonable probability that another

87. Dhillon, *supra note 26* at 150.

88. Smith *supra note 20*. For further discussion of the implications of *Smith* for seizure of electronic communications, see the Department of Justice search and seizure manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice (January 2001), available at http://www.usdoj.gov:80/criminal/cybercrime/searchmanual.wpd (last visited January 24, 2002).

89. Dhillon *supra note 26*, at 150.

90. US Const. amend. IV.

91. Petti *supra note 56*, citing Maryland v. Garrison, 480 U.S. 79, 84, 94 L. Ed. 2d 72, 107 S. Ct. 1013 (1987).

premise might be mistakenly searched," it is in compliance with the Fourth Amendment.[92] A court order to tap all phones used by a specific person *does* describe particular places, but in an unconventional way. Public authorities cannot use the order to tap any location they wish, but only a set of specific locations, which they can show are used by a specific person.[93]

Not everyone agrees that this substitution of particularity of person for particularity of place is sufficient to satisfy the Fourth Amendment. Tracey Maclin cites the Supreme Court case of *Steagald v. United States* in which the Court concluded that an arrest warrant that specifies a person cannot be used to search private places not named in the warrant in pursuit of that person.[94] She interprets this decision to mean that the Court found warrants to be flawed that specify only the target of the search, but leave police to determine which particular locations to search. Maclin argues that although roving intercepts are issued for one person, once public authorities decide to "tap" a telephone or computer, everyone using that telephone or computer will be subject to surveillance, so there is no true particularity of person maintained.[95]

In his analysis of the issue, Clifford Fishman finds that although relevant Fourth Amendment case law does not give conclusive support either for or against roving intercepts, there are strong arguments in favor of their constitutionality. He holds that roving intercept orders "describe the 'place' to be searched in a somewhat untraditional, but still sufficiently particular way" and argues that "if the Fourth Amendment is flexible enough to protect privacy against technological developments far beyond the contemplation of the founding fathers, then it

92. *Id.* citing United States v. Turner, 770 F.2d 1508, 1510 (9th Cir. 1985).

93. The United States code specifies that in the case of a roving intercept "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." 18 USC 1518 (11)(b)(iv); and that the interception "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." 18 USC 1518 (12).

94. Steagald v. United States, 451 U.S. 204 (1981).

95. Tracey Maclin, *Another grave threat to liberty*, NAT'L L. J., Nov. 12, 2001, A20.

must also be flexible enough to permit investigators to preserve the basic mandate of the amendment's particularity requirement in a novel way."[96]

Numerous additional questions arise regarding the difference in applying the new laws, as well as the old ones, to non-citizens vs. citizens, to terrorists vs. criminals, and to international vs. domestic terrorists. These are huge issues that concern the extent to which the Constitution applies to non-citizens, in the United States and elsewhere, and what rights non-citizens have. These issues raise potential problems, such as how to define terrorism and whether that definition should extend to citizens, as well as the danger that a loose definition might allow ordinary criminals to be encompassed by terrorism laws. These issues go well beyond communications technology and the laws related to it–the focus of this article–and are not covered here, although they have implications for the issues at hand.

c. Other critiques

Proponents of roving intercepts argue that without them authorities will see a "whole operation frustrated because a terrorist throws away a telephone and picks up another phone and then moves on."[97] Critics argue that the new law will ensnarl many innocent people unrelated to investigations. Civil libertarians like Nadine Strossen argue that the new law, as it relates to roving intercepts, "goes far beyond" facilitating investigations based on individual suspicion. She uses the example of a suspected terrorist who sends e-mail from a public library computer terminal. If the computer is tapped, any of the other users, who have no connection to the suspect, will also have their communications intercepted.[98] The same critics contend that issuing nationwide warrants just allows law enforcement agents to "shop for friendly judges."[99] Senator

96. Clifford S. Fishman, *Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1 (Fall 1987) [hereinafter Fishman], at 65-69.

97. Solicitor General Ted Olsen, on CNN, *Larry King Live*, Oct. 24, 2001.

98. Nadine Strossen, on CNN News, International. Oct. 30, 2001.

99. Bart Kosko, *Your Privacy is a Disappearing Act*, LOS ANGELES TIMES, Dec. 2, 2001, at M5

Hatch counters that these provisions and others merely fix parts of the criminal code that formerly treated terrorists "with kid gloves."[100]

It is worth noting that although the ACLU does not exempt the laws at issue from its blanket criticism of all the new measures, when explicitly asked whether it would at least recognize that allowing public authorities to tap all phones used by the same person was eminently reasonable, it hinted that it is somewhat less troubled by the changes in the laws under discussion here than by many of the other measures.[101] Alan Dershowitz, a longtime defender of civil liberties, even went so far as to concede that roving intercepts are "a very good idea."[102]

The ACLU criticizes changes in FISA, which it charges allow authorities to "by-pass normal criminal procedures that protect privacy and take checks and balances out of the law."[103] Civil libertarians worry about USA Patriot's extension of the reach of FISA, which provides fewer protections than are provided for criminal cases, as the discussion above regarding full intercepts under FISA illustrates. (Civil libertarians' concerns about pen/trap orders for e-mail are discussed in the section on protective technologies.)

***

I shall defer my own assessment of the legitimacy of the new legal adaptations to the liberalizing technologies and of their effects on the balance between individual rights and public safety and health, until the next three technologies and the laws concerning them are reviewed. For now it might serve to remind that the essay does not deal with the general legitimacy of FISA or the USA Patriot Act, but with some elements of these laws, specifically those that concern communications surveillance. This is significant to keep in mind because conclusions about other elements–military tribunals and indefinite detention of suspects, for instance–may be different than those about the surveillance laws at issue.

---

100. Adam Clymer, *Anti-terrorism bill passes, U.S. gets expanded powers*, NYTIMES, Oct. 26, 2001, at A1

101. Strossen remarks, *supra note 4.*

102. Alan Dershowitz, on CNN NEWS, INTERNATIONAL. Oct. 30, 2001.

103. *The USA-PATRIOT ACT Boosts Government Powers While Cutting Back on Traditional Checks and Balances.* (ACLU, Leg. Analysis) available at http://www.aclu.org/congress/l110101a.html (last visited Jan. 17, 2002).

II. PUBLIC PROTECTIVE TECHNOLOGIES

The discussion now turns to three technologies that have the opposite profile of those explored so far: they enhance the capabilities of public authorities and raise fears that they will curtail individual rights.

A. Carnivore

Carnivore, a computer program that was unveiled by the FBI in July of 2000, is used to trace and seize Internet communications. To capture a suspect's messages or trace messages sent to and from his account, public authorities must sort through a stream of many millions of messages, including those of many other users as well as those of the suspect. Some ISPs have the capability of doing this sorting themselves and will simply pass the appropriate information on to agents after a warrant or court order is presented. If an ISP is not capable of doing this kind of sorting, the FBI uses Carnivore to do it.[104]

Carnivore runs as an application program on an operating system and works by screening e-mails and sorting them based on a "filter," which tells the program which information to capture and which to merely let pass by. The filter can be set to sort out messages from a specific computer or e-mail address, or it can scan various packets to find a specific text string.[105] Carnivore can be set to operate in two different modes: "pen" and "full." In pen mode it will capture only the addressing information (which includes the e-mail addresses of the sender and recipient, as well as the subject line) while in full mode it will capture the entire content of a message.[106] Carnivore is designed to copy and store only information caught by the filter, thus

104. Letter from Assistant Director John Collingwood to Members of Congress (Aug. 16, 2000), available at http://www.fbi.gov/congress/congress00/collingwood081600.htm (last visited Jan. 29, 2002).

105. Illinois Institute of Technology Research Institute, *Independent Review of Carnivore System- Final Report* (2000), available at http://www.epic.org/privacy/carnivore/carniv_final.pdf (Last visited Jan. 29, 2002) [hereinafter IITRI Report], at 3.4.4.1.1, 3.4.4.1.4, 3.4.4.1.6

106. *Id.* at 3.4.4.1.3.

keeping agents from looking at any addressing information or e-mail content not covered in the court order.[107]

Carnivore's pen mode is of value to public authorities even if the messages themselves cannot be read, such as in the growing number of cases in which high power encryption is used, because the government benefits from an analysis of the addresses. For instance, it can use pen/trap orders to trace to whom a group of suspects address their e-mail. When used in this capacity, it would make more sense to call Carnivore (which hardly devours the messages, despite its name) a communications traffic analyzer.

As of the fall of 2000, the FBI said that it had used Carnivore "approximately 25 times in the last two years."[108] The Carnivore program is stored in an FBI laboratory and only brought out when needed to fulfill a specific court order. After the court order has expired, the program is returned to the laboratory.[109]

B. The Key Logger System and Magic Lantern

Despite the introduction of Carnivore, the government seems to be greatly hobbled by its inability to decrypt a rapidly growing proportion of all messages. To overcome this limitation, the FBI is introducing two new technologies to obtain a suspect's password. A password can enter or exit the encryption/decryption process in four ways: going over a modem, retrieval from storage, entry into a keyboard, or a process working within the computer itself.[110] The Key

107. *Fourth Amendment Issues Raised by FBI's "Carnivore" Program: Hearing Before the House Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 1 (2001) (statement of Donald M. Kerr, Assistant Dir. Lab. Div. FBI) [hereinafter July 2000 Kerr statement].

108. *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing before the Senate Comm. on the Judiciary*, 106th Cong. 3 (2000) (statement of Donald M. Kerr, Assistant Dir. Lab. Div. FBI) [hereinafter Sept. 2000 Kerr statement].

109. July 200 Kerr statement, *supra note 107*.

110. Aff. of Randall S. Murch, United States District Court District of New Jersey, United States v. Scarfo (Oct. 4, 2001), available at http://www.epic.org/crypto/scarfo/murch_aff.pdf (last visited Jan. 29, 2001) [hereinafter Murch Aff.].

Logger System (KLS), developed by the FBI, has several components that work together to obtain someone's password.[111]

Once agents discover that information they have seized through a warranted search or intercepted with a proper court order is encrypted, they can obtain another warrant to install and retrieve the KLS.[112] In the case of Nicodemo Scarfo, who was suspected of racketeering, agents had to show both probable cause that Scarfo was involved in crime and probable cause that important information was installed on his computer in encrypted form. As in any warrant, the FBI had to specify the exact location of the computer on which the KLS would be installed.[113]

Once installed, the KLS uses a "keystroke capture" device to record keystrokes as they are entered into a computer. It is not capable of searching or recording fixed data stored on the computer, or of intercepting electronic communications sent to and from the computer (which would require an intercept order, which is more difficult to get than a warrant). In order not to intercept inadvertently the content of communications, the KLS is designed so that it is unable to record keystrokes while a computer's modem is in operation.[114]

Because the KLS must be installed manually and covertly on a suspect's computer, which involves breaking and entering, it is arguably more invasive than "back doors" and key escrow (which, as previously discussed, are not available, due mainly to opposition by civil libertarians and high-tech business interests).[115] Those who are shocked by this technology should consider the effects of high power encryption. As the *Boston Globe's* technology reporter commented,

---

111. In his affidavit during the Scarfo trial, FBI's Randall Murch explains that the public encryption key is usually a long string of computer data that the user cannot simply memorize. Instead, the user has a passphrase that enables him to decrypt his files. When the passphrase is entered into a dialog box, the program then decrypts the key and then uses it to decrypt the file. *Id.*

112. *Judge Orders Government to Explain How "Key Logger" System Works*, COMPUTER AND ONLINE INDUSTRY LITIGATION REPORTER, Aug. 14, 2001, 3.

113. Order to search Merchant Services of Essex County, filed May 8, 1999. United States Court District, District of New Jersey, available at http://www2.epic.org/crypto/scarfo/order_5_99.pdf (last visited Jan. 29, 2001) [hereinafter Scarfo warrant].

114. The component that records the keystrokes can be set to evaluate each keystroke individually before recording it. When a keystroke is entered, KLS checks the status of the computer's communication ports. The component will only record a keystroke if all the communications ports are inactive. Murch Aff., *supra note 110*.

115. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (Jan. 1995).

"techno-libertarians rightly howled when the feds tried to bar access to encryption software; now we must live with the consequences. The bad guys have encryption. The good guys must have counter-encryption tools."[116]

Recently, the FBI has revealed that it has been developing a less invasive technology. In November 2001, the FBI admitted that it had developed, but not yet implemented, a remote-control approach called Magic Lantern that allows the FBI to put software on a computer that will record keystrokes typed without installing any physical device.[117] Like the KLS, Magic Lantern does not by itself decrypt e-mail, but can obtain the suspect's password. The details of how it does this have not been released.[118] It is said to install itself on the suspect's computer in a way similar to a Trojan horse computer virus. It disguises itself as ordinary, harmless code, then inserts itself onto a computer. For example, the FBI will have a box pop up when someone connects to the Internet reading something like "Click here to win." When the user clicks on the box, the virus will enter the computer.[119]

C. Evaluating the new technologies

Just as laws were put in place both before and after 9/11 to limit the concerns that new liberalizing technologies posed for public safety, measures have also been introduced that limit the use of new protective technologies and address the concerns they pose for individual rights. Most of the limitations on the use of Carnivore and the KLS were put in place as these technologies developed and before they were used, though there have also been "additions" to the checks placed on them. The shift from the KLS to Magic Lantern can be considered an improvement from a rights viewpoint because it will not require covert breaking and entering by a law enforcement agent to install it on a suspect's office or home computer.

---

116. Hiawatha Bray, *Military-Tech Complex*, BOSTON GLOBE, Nov. 29, 2001, at C1.

117. Ted Bridis, *FBI develops new tools to ensure government can eavesdrop on high-tech messages*, ASSOCIATED PRESS, Oct. 21, 2001.

118. Bob Port, *Spy Software Helps FBI Crack Encrypted Mail*, DAILY NEWS, Dec. 9, 2001, at 8.

119. Lou Doliner, *With new tools, authorities can target suspects' computers with accuracy*, NEWSDAY, Dec. 12, 2001, at C08.

Nevertheless, both Carnivore and the KLS have raised concerns on the part of privacy advocates and civil liberties groups. Critics are skeptical that the programs operate the way the FBI claims they do and are troubled by the degree of secrecy the FBI maintains regarding how the programs work.

Groups like the Electronic Privacy Information Center (EPIC) and the Center for Democracy and Technology (CDT) have multiple arguments for why Carnivore should not be used at all. They argue that because, for e-mail, it is much harder to separate addressing information from content than for a phone call, Carnivore will not allow the FBI to do a pen/trap without seizing more information than authorized.[120] Privacy advocates also worry that Carnivore will scan through "tens of millions of e-mails and other communications from innocent Internet users as well as the targeted suspect,"[121] thus violating the Fourth Amendment.[122] The ACLU compares a Carnivore search to the FBI sending agents into a post office to "rip open each and every mail bag and search for one person's letters" and to "tapping the entire phone exchange system, listening to all the conversations, and then keeping only the ones that are incriminating, instead of tapping a single phone line."[123] A *USA Today* editorial stated that "once it's in place, Carnivore acts as an unrestrained Internet wiretap, snooping through every Internet communication that comes within its reach."[124]

Officials at the FBI respond that Carnivore, when it is used properly, will pull out only the appropriate e-mails, and that its use is subject to strict internal review and requires the cooperation of technical specialists and ISP personnel, thus limiting the opportunities an

---

120. *Hearing on Protecting Constitutional Freedoms from Infringement by Counterterrorism Efforts Before the Subcomm. on the Constitution, Federalism, and Property Rights of the Sen. Comm. on the Judiciary Committee*, 107th Cong. (2001) (statement of Jerry Berman, Exec. Dir. Center for Democracy and Technology) [hereinafter Berman statement].

121. See ACLU, Urge Congress to Stop the FBI's Use of Privacy-Invading Software (2000), available at http://www.aclu.org/action/carnivore107.html (last visited January 10, 2002) [hereinafter ACLU].

122. See Aaron Kendal, *Carnivore: Does the Sweeping Sniff Violate the Fourth Amendment?*, 18 T.M. COOLEY L. REV. 183 (Trinity Term 2001).

123. See ACLU, *supra note 121*.

124. *FBI eavesdrops on e-mail, crashed privacy barriers*, USA TODAY, July 24, 2000, at 16A.

unscrupulous agent might have to abuse it. In Donald Kerr's words, the FBI does not have "the right or the ability to just go fishing."[125]

A review of Carnivore conducted by the Illinois Institute of Technology concluded that although it does not completely eliminate the risk of capturing unauthorized information, Carnivore is better than any existing alternatives and should continue to be used.[126] However, the panel also determined that the FBI's internal audit process is insufficient to protect against improper use.[127] Specifically, the operator implementing a Carnivore search selects either pen or full mode by clicking one box on a computer screen,[128] and because the program does not keep track of what kind of search has been run,[129] it is difficult to determine if an operator has used the program only as specified in the court order. The head of the panel commented: "Even if you conclude that the software is flawless and it will do exactly what you set it to do and nothing more, you still have to make sure that the legal, human and organizational controls are adequate."[130] I turn to this matter below, when accountability is discussed.

There is a tendency to attribute to computers human attributes and talk or write about them as if they "sniff" and "snoop," violate privacy, and so on. One day computers may achieve such human capabilities, but for now a computer does not ogle, snicker at, or get aroused by a picture of a nude person because it does not "see"; its "mind" processes merely ones and zeros. Thus, if millions of messages flow through a computer running Carnivore, none of them is "read" *unless* it is caught by the filter and passed on to a human observer.[131] Computers do not "read" or "scan" messages any more than phones "listen" to messages left in their voice mail box. The issue is what humans do–not machines. True, if new technological capabilities did not

---

125. Tom Bridis, *Congressional Panel Debates Carnivore as FBI Moves to Mollify Privacy Worries*, THE WALL STREET JOURNAL, July 25, 2000, at A28.

126. IITRI Report, *supra note 105*, at ES.5 - E.S.6.

127. *Id.* at ES.5.

128. *Id.* at xi and xiv.

129. *Id.* at ix, xiii.

130. John Schwartz, *Wiretapping System Works On Internet, Review Finds*, NY TIMES, Nov. 22, 2000, at A19.

131. IITRI Report, *supra note 105*, at 3.4.4.1.

exist or their use were fully banned–an old Luddite argument[132]–the problem would not arise in the first place. However, as long as new technologies are available to criminal elements, it is hard to argue in favor of privileging them and blocking the government from using counter-measures under the proper conditions.

The legality of the KLS was tested in the case of Nicodemo Scarfo, in which the FBI used the KLS to decrypt records implicating Scarfo in racketeering. Scarfo's defense argued that the key logger records keystrokes typed in electronic communications and sent over a modem, and should therefore have required a full intercept order, rather than an easier to obtain search warrant. Though the FBI says that the KLS cannot record while a modem is in operation, thus protecting against the capture of electronic communications, Scarfo and the privacy advocates interested in the case were skeptical. During the trial, Scarfo was shown a hard copy of all of the keystrokes intercepted, but was unable to pick out anything that he recognized as being part of an electronic communication.[133]

Scarfo also argued that the warrant used to install the KLS violated the particularity requirement of the Fourth Amendment and therefore constituted a general search because it did not describe specifically what could be searched and seized.[134] The warrant in the case authorized FBI agents to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION," which was specified in great detail. The same warrant authorized the surreptitious breaking and entry into the target location to install and retrieve the KLS, and also authorized the FBI to seize business records "in whatever form they are kept."[135] David

132. For an example of the Neo-Luddite position, see Chellis Glendinning, *Notes Toward a Neo-Luddite Manifesto*, UTNE READER, Mar./Apr., 1990. For an historical discussion of Luddism, see KIRKPATRICK SALE, REBELS AGAINST THE FUTURE (1995).

133. Brief of the United States in Opposition to Defendant's Pre-trail Motions, United States v. Scarfo, (July 2001) Available at http://www2.epic.org/crypto/scarfo/gov_brief.pdf (last visited January 29, 2002) [hereinafter Scarfo brief].

134. Motion to Suppress Evidence Seized by the Government Through the Use of a Keystroke Logger, United States v. Scarfo, (June 2001), available at http://www2.epic.org/crypto/scarfo/def_supp_mot.pdf (last visited Jan. 29, 2002).

135. Scarfo warrant, *supra note 113*.

Sobel of EPIC said that since the warrant was issued to get one password, but the KLS recorded every keystroke typed, it was comparable to if a police officer got "a warrant to seize one book in your house, but was also allowed to haul out everything that's in there."[136] Although it is true that in the Scarfo case agents had to look through all keystrokes entered after the installation of the KLS in order to pick out the string that was his password, the FBI argues that this is similar to any search. If public authorities have a warrant to get someone's account book from their office, they may have to look through many drawers and shelves before finding it.[137] In December of 2001, the judge in the Scarfo case ruled that the use of the KLS to obtain his password was legal and constituted neither a general search nor a form of surveillance.[138]

III. ACCOUNTABILITY

A. Accountability, the second balance

The article opened by calling attention to the need for balance between individual rights and public safety and health, rather than one or the other predominating. When the polity tilts too far toward safety or rights, such tilts are best corrected. The question hence arises what effects the new technologies have on the balance. There can be little doubt that (a) the liberalizing technologies have greatly hindered the work of public authorities in the area of communications surveillance; (b) new protective technologies to some extent overcome these difficulties. The same might be said (c) about new legislation that did adapt the old applicable laws to the new technologies. Finally (d) the 2001 attack on America changed the point (or zone) of balance by posing a new, credible threat to public safety and health. This still leaves open the question of whether the new measures, whether technological or legal, provide for much needed enhanced public safety or excessively intrude into individual rights.

This, in turn, raises the question of how generally to determine whether or not the polity is in the zone of balance. This is an issue with which the courts have struggled for generations; it

136. Richard Willing, *FBI technology raises privacy issues*, USA TODAY, July 31, 2001, at 3A.

137. Scarfo brief, *supra note 133*, at 38.

138. Opinion and Order in the case of United States v. Scarfo et al., issued Dec. 26, 2001, available at http://lawlibrary.rutgers.edu/fed/html/scarfo2.html-1.html (last visited Jan. 29, 2002).

would take volumes to begin to do it justice. Also, I have dedicated some text to this issue elsewhere.[139] Briefly, I concluded that the course of a nation's laws should not be corrected unless there is a compelling reason (a concept akin to "clear and present danger," although not necessarily one that meets this criterion technically); unless the matter cannot be addressed by non-legal, voluntary means; and unless one can make the intrusion small and the gain (either in safety or in rights) considerable. Further specification draws on what a reasonable person would find sensible, taking into account that the Constitution is a living document whose interpretation has been adjusted through the ages.

These criteria can be applied to the issues discussed here. For example, in the post-9/11 context, it is clear that the government should have greater powers to decrypt e-mail because: terrorism does pose a major threat; voluntary means to fight encrypted terrorist messages have not sufficed on the face of it; and enabling and allowing the government to decrypt e-mail messages is not more intrusive than tapping a phone and can be allowed under similar conditions. The authority to use roving wiretaps may pass the same test. (To reiterate, other public safety measures recently introduced that do not concern communications surveillance, such as requiring protestors to remove their disguises, are not discussed here and may very well not meet the criteria listed.)[140]

To complete the judgment whether or not a given new measure that enhances the powers of public authorities is called for, I suggest that *a second form of balancing needs to be considered* that, arguably, in the matters at hand, may turn out to be decisive compared to the first form already discussed. It concerns not whether the government should be accorded new powers—but *how closely it is held accountable regarding the ways it uses these powers*. From this viewpoint, the key issue is not if certain powers–for example, the ability to decrypt e-mail–should or should not be available to public authorities, but whether or not these powers are used legitimately and whether mechanisms are in place to ensure such usage. This is similar to passing

139. AMITAI ETZIONI, THE SPIRIT OF COMMUNITY: THE REINVENTION OF AMERICAN SOCIETY (1993), chap. 6, The New Golden Rule, *supra note 6*, chaps. 1 and 2.

140. *The Economist* reports that the anti-terrorism bill released by the United Kingdom's home secretary David Blunkett on November 13 includes a provision that would give public authorities the power to force protestors to remove disguises. THE ECONOMIST, Nov. 17, 2001, at 54.

over the question of whether there is too much money in a vault in favor of asking how strong the locks are. (One may argue that, in effect, this is really one question because whether the sum is "too much" depends on the locks. Some would argue that whatever the quality of the locks, too much of one's money should not be located in one bank, mutual fund, etc. This is surely the argument about government data banks. However safeguarded, libertarians oppose concentrated national databases.)

Although these two forms of balance have some similarities and points of overlap, they are quite distinct. Thus, to argue, as cyber-libertarians did, that the government should not be able to decrypt encoded messages, should not be allowed to demand from an ISP the addressing information for e-mail sent to and from a suspect's account, and so on, is different from agreeing that such powers are justified *so long as they are properly circumscribed and their use is duly supervised.*

The balance sought here is not between the public interest and rights, but between the supervised and the supervisors. Deficient accountability opens the door to government abuses of power; excessively tight controls make for agents reluctant to act.

Thus, a case can be made that in the decades preceding the Church Commission, under most of Hoover's reign, the FBI was insufficiently accountable, and that after the Commission's rules were institutionalized, until 9/11, the FBI was excessively limited in what it was allowed to do, in the area of communications surveillance. Agents, fearing reprimands and damage to their careers, were often too reluctant to act.

To elaborate a bit: It seems difficult to sustain the argument that the government should be unable to decrypt any messages or be unable to gain the authority to do so. After the first bombing of the World Trade Center in 1993, one of its principal masterminds used encryption to protect files on his laptop computer, even as he plotted to blow up commercial airlines.[141] (Encrypted files were found on a computer used by Osama bin Laden's lieutenants in the Afghan capital.[142]) Few would argue that public authorities should be unable to decrypt such files, even,

---

141. *Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the House Appropriations Committee, Subcommittee on Commerce, Justice, State, Judiciary and Related Agencies,* 105th Cong. (1998) available at http://www.fbi.gov/congress/congress98/hac35.htm (last visited Jan. 29, 2002).

142. Alan Cullison and Andrew Higgins, *How al Qaeda Agent Scouted Attack Sites In Israel and Egypt*, THE WALL STREET JOURNAL, Jan. 16, 2002, at 1.

say, after obtaining a warrant based on probable cause that the files included important information.

The issue hence becomes which limits will be set on what messages can be decrypted, who will verify that these limits are observed, and by what means. Similarly, regarding roving intercepts, the issue is not whether the government should have to get a warrant for each instrument of communication that the same suspect uses, but by what means it will be ensured that the government does not collect information about other people who use the same instruments of communication or the same computer terminal. The key issue is not whether communications in cyberspace should be exempted from the same type of public scrutiny to which mail and phone calls have historically been subject, as cyber-idealists had hoped,[143] but whether there are proper controls in place to protect against abuse.

The next step in assessing whether or not the American polity, in matters concerning communications surveillance, is currently excessively attentive to public safety or not willing to take needed measures out of excessive concern for rights, is hence to determine to what extent accountability has been built into the new powers granted to the government in response to the new technologies at hand and in reaction to 9/11.

B. Layers of accountability

1. Limitations built into the law

Limitations on the use of new powers are written into the laws governing them and limitations on protective technologies are often built into the technologies themselves. Roving intercepts, and indeed any intercepts, are not granted without limits. Title III lays out a requirement for "minimization," stated at follows: "Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."[144]

143. Levy, *supra note 45*, chap 7.

144. 18 USC 1518 (5).

Such built-in guidelines are intended to limit the ability of public authorities to gather and use information not directly related to their investigations.[145] Practically, this means that agents are not allowed to record conversations that are unrelated to the subject of the investigation and should stop listening when irrelevant matters are being discussed. If agents are unsure if a seemingly innocent conversation might touch on a relevant subject at some point, agents are to conduct "spot-monitoring," in which they tune in every few minutes to check, but only begin to record when appropriate.[146]

In *Scott v. United States*,[147] the Supreme Court found that an agent's implementation of such guidelines must be evaluated under a "standard of objective reasonableness," so that if circumstances make minimization difficult, failure by an agent to attempt it does not constitute a violation of the law[148]. In addition, if investigators have reason to suspect a conspiracy involving a large number of people, they are justified in recording and listening to all conversations until they are certain who is innocent and who not.[149] Many critics point out that under any circumstances, minimization is voluntary and we must rely on our trust in law enforcement officers to do it properly, highlighting the importance of further layers of accountability, such as the exclusionary rule.[150]

Although telephone wiretaps rely on human judgment in implementing minimization, new public protective technologies, if properly used, carry out much of the minimization function automatically. Carnivore's filters, if set properly, act as a built-in minimization process, intercepting only what is appropriate. Although it might be capable of collecting all content that passes through it, in compliance with court orders it should be set to capture only data sent to and

145. 18 U.S.C. 2518 (5) (Supp. IV 1986).

146. *See, e.g.*, United States v. Clerkley, 556 F.2nd 709, 717 (4th Cir. 1977); United States v. Costello, 610 F. Supp. 1450, 1477 (N.D. Ill. 1985); United States v. Clemente, 482 F. Supp. 102. 108-10 (S.D.N.Y. 1979).

147. Scott v. United States, 436 US 128 (1978).

148. *Id.* at 137-39.

149. *Id*. at 142.

150. The Honorable Bob Barr, A Tyrant's Toolbox: Technology and Privacy in America, 26 J. LEGIS. 71 (2000).

from a specific user.[151] As mentioned before, data that does not fit the filter settings just passes through without being saved by Carnivore, and is therefore not seen by public authorities.[152]

2. Supervision within executive agencies

Numerous accountability mechanisms are built into the executive agencies of the government. Of course, FBI field agents are subject to numerous guidelines and supervisors whose job includes ensuring that these guidelines are abided by. They, in turn, report to still higher ranking supervisors. Moreover, when agents cross the line, internal reviews take place. In addition, the Attorney General's office to some extent supervises what the FBI does.

For instance, as already mentioned, requests by the FBI to conduct communications surveillance under FISA must be approved by the Attorney General's office before they are submitted to the FISC. In some cases, court order or warrant requests never get past internal FBI approval procedures. For example, in the investigation prior to 9/11 of Zacarias Moussaoui, the possible "20th hijacker" who did not make it onto an airplane because he was arrested before 9/11 on immigration charges, the request by field agents to search his computer never made it past FBI attorneys, who found insufficient evidence to justify it.[153]

3. The courts

Once surveillance technology is available that makes possible such actions as scanning e-mail or gaining to keys to decrypt messages, and once it is established in principle that the government will have access to such technology, the question for both sides becomes–under what conditions should the government be allowed to use it? Often the contest on this second level issue centers on the issuance of warrants and court orders.

Civil libertarians hold that court orders are issued too liberally, without due scrutiny. They argue that agents cannot be trusted to abide by minimization guidelines, so it is best not to

151. IITRI Report, *supra note 105*, at 3.4.4.1.6, ES.5.

152. *Id.* at 3.4.4.1.3.

153. Dan Eggen and Brook Masters, *U.S. Indicts Suspect in September 11 Attack*, WASHINGTON POST, Dec. 12, 2001, A01.

grant them court orders in the first place. Jerry Berman stated that some 1,000 intercept orders a year are approved under FISA, suggesting that this is a very large number.[154] In fact, only around 10,000 intercept orders have been granted under FISA since its creation in 1979,[155] amounting to fewer than 1,000 a year.

Civil libertarians point to the fact that the FISC has only denied one request for surveillance in its entire history as evidence that the standards for receiving a FISA intercept order are lower than for receiving a Title III order.[156] Though applications for intercept orders are rarely turned down by the FISC, public safety advocates point out that it is embarrassing and damaging to one's record and career to be turned down by the FISC, and as a result agents are reluctant to request warrants even when they seemed justified.[157] Moreover, if the FISC finds that there is not sufficient justification, it tends to return the request for further documentation rather than denying the request outright, which accounts for there being next to no outright refusals.[158] As mentioned above, some requests never get past the Attorney General's office. Also, FISA applications need to meet preset guidelines and must include a statement of the means by which the surveillance will be conducted, as well as a statement of proposed minimization procedures.[159]

Although civil libertarians typically are much more favorably disposed toward courts than toward the administrative parts of the government, they fear that judges might be unable or disinclined to curb law enforcement agents.[160] First, judges are either elected or politically appointed, making them subject to the influence of public opinion, especially since 9/11. In

154. Berman statement, *supra note 120*.

155. William Carlson, *Secretive US Court may add to power*, SAN FRANCISCO CHRONICLE, Oct. 6, 2001, at A3.

156. Berman statement, *supra note 120*.

157. Private communication with Orin Kerr, Washington, DC, Dec. 14, 2001.

158. Toensing remarks, *supra note 25*.

159. 50 USC 1804(a).

160. "Law enforcement, rather than a Court, will decide what is "content" and systems like Carnivore will be used without any real judicial supervision." ACLU, *More on ACLU Objections to Select Provisions of Proposed Anti-Terrorism Legislation*, (2001) available at http://www.aclu.org/congress/Patriot_Links.html (last visited Jan. 17 2002).

addition, it has been suggested that judges are less accountable outside their home jurisdictions and might thus be less cautious in granting, and less diligent in enforcing proper implementation of, warrants and court orders they issue that apply to other jurisdictions, as allowed by the USA Patriot Act. Judge Meskill, in his concurrence with the ruling in *United States v. Rodriguez*, warned that "judges may be more hesitant to authorize excessive interceptions within their territorial jurisdiction, in their own back yard so to speak, than in some distant, perhaps unfamiliar, part of the country. Congress determined that the best method of administering intercept authorizations included territorial limitation on the power of judges to make such authorizations."[161] If this is true, it would weaken the courts as an accountability mechanism for nationwide warrants.

In addition to the requirements that need to be met to get a warrant or court order in the first place, courts ensure that law enforcement agents act within the limits of the power granted to them by suppressing evidence that is collected illegally. The exclusionary rule–that evidence collected in violation of the Fourth Amendment must be excluded from a trial against the suspect–was not originally written into the Constitution, but was established in the Supreme Court case *Boyd v. United States*[162] and later re-affirmed in *Weeks v. United States*.[163] It has since been diluted in more ways than one.[164] Still, evidence collected illegally will be suppressed. This serves not only to protect the suspect after a violation occurs, but also to deter inappropriate searches because agents know that if they do not follow the correct procedures, the culprits might go free.

---

161. *United States v. Rodriguez*. 968 F. 2d 130, 135 (2d Cir. 1992).

162. Boyd v. United States, 116 U.S. 616 (1886).

163. Weeks v. United States, 232 U.S. 383 (1914).

164. *See e.g.* United States v. Leon, 468 U.S. 897 (1984), which established a "good faith" exception to the exclusionary rule; Nix v. Williams, 467 U.S. 431, 444 (1984), which created the "inevitable discovery" exception to the exclusionary rule; Massachusetts v. Sheppard, 468 U.S. 981 (1984), upholding the "good faith" exception; United States v. Calandra, 414 U.S. 338, 348 (1974), which establishes that the exclusionary rule does not proscribe use of *all* illegally obtained evidence. For further discussion, see Leslie-Ann Marshall and Shelby Webb, Jr. *Constitutional Law -- The Burger Court's Warm Embrace Of An Impermissibly Designed Interference With The Sixth Amendment Right To The Assistance of Counsel -- The Adoption Of The Inevitable Discovery Exception To The Exclusionary Rule: Nix v. Williams.* n1, 28 HOW. L.J. 945 (1985); Christopher A. Harkins, *The Pinocchio Defense Witness Impeachment Exception to the Exclusionary Rule: Combating a Defendant's Right to Use With Impunity the Perjurious Testimony of Defense Witnesses*, 1990 U. ILL. L. REV. 375 (1990), at 389-411.

4. Congress

Under our system of checks and balances, Congress, of course, is supposed to oversee the work of the executive branch and its agencies. It has many instruments for doing so, including requiring heads of agencies and other high ranking officials to respond to written questions, testify before congressional committees, and turn over documents; conducting hearings in which civil libertarians and others can make their case; ordering the General Accounting Office to conduct a study; and more.

A survey of the extent to which Congress provides another layer of accountability regarding issues such as those covered here, above and beyond what is provided by the agencies themselves and by the courts, is well beyond the scope of this article. It should be noted, though, that civil libertarians argue that many of the measures included in USA Patriot (including those explored here) were enacted in a great rush, without the usual hearings and deliberations.[165] Supporters of the public authorities point out that after 9/11 it was assumed that there were other "sleeper" terrorist agents in the United States and that other attacks were imminent, and argue that therefore the rush was justified. Indeed, they held that expanded powers should have been given well before 9/11.[166] Moreover, hearings and other reviews of the issues at hand, such as Carnivore, were conducted before 9/11.[167]

---

165. "The process that brought you this bill is terribly flawed. After bypassing a Judiciary Committee mark-up, a few Senators and their staffs met behind closed doors, on October 12, 2001 to craft a bill. The full Senate was presented with anti-terrorism legislation in a take-it-or-leave-it fashion with little opportunity for input or review. No conference committee met to reconcile the differences between the House and Senate versions of the bill. We find it deeply disturbing that once again the full Senate will be forced to vote on legislation that it has not had the opportunity to read. Senate offices are closed and staff cannot even access their papers to fully prepare you for this important vote. Regular order is being rejected and it is an offense to the thoughtful legislative procedures necessary to protect the Constitution and Bill of Rights at a time when the rights of so many Americans are being jeopardized."

Letter from Laura Murphy, Dir. ACLU Wash. Office to Senate, Urging Rejection on Final Version of USA Patriot Act, Oct. 23, 2001, available at http://www.aclu.org/congress/1102301k.html (last visited Jan. 17, 2002).

166. Sen. Orin Hatch said before Congress that:

"We can never know whether these tools would have prevented the attack on America, but, as the Attorney General has said, it is certain that without these tools we did not stop the vicious acts of last month. I personally believe that if these tools had been in law--and we have been trying to get them there for years--we would have caught those terrorists. If these tools could help us now to track down the perpetrators--if they will help us in our continued pursuit of terrorists--then we should not hesitate to enact these measures into law. God willing, the legislation we pass today will enhance our abilities to protect and prevent the American people from ever again being violated as we were on September 11."

5. The public

The ultimate source of oversight is the citizenry, informed and alerted by a free press and civil liberties advocates and briefed by public authorities about their needs. To be fully effective in overseeing the issues at hand, civil libertarians argue that the public must be informed about the inner workings of the protective technologies, while public authorities claim that such disclosures would inform terrorists and other criminals about how to circumvent the technologies, thus rendering them useless. Specifically, since the existence of Carnivore was made public, numerous parties have demanded access to information about how it works. The ACLU filed a Freedom of Information Act (FOIA) request to get its source code, which reveals what a program is intended to do and how it operates.[168] The Electronic Privacy Information Center, a privacy advocacy group, filed an FOIA request to gain a copy of *all* documents relating to Carnivore.[169] In addition, numerous ISPs who might be asked to cooperate in installing Carnivore wanted guarantees that the program worked as claimed and that there would be sufficient controls to keep law enforcement agents from capturing more than what was covered in the court order.[170]

In the Scarfo case, the judge joined civil liberties groups in demanding that the FBI release information on how the KLS works, arguing that he could not rule on whether or not its use was legal without knowing how the technology worked. The judge said he would review the

---

CONG. REC. S11015 (2001) (statement of Sen. Hatch).

167. The House Judiciary Committee held a hearing on the Fourth Amendment Issues Raised by the FBI's Carnivore Program on July 24, 2000. Testimonies are available at http://www.house.gov/judiciary/con07241.htm, (last visited on January 22, 2002). The Senate Judiciary Committee held a hearing on Carnivore on Sept. 6, 2000. Testimonies are available at http://www.senate.gov/~judiciary/wl96200f.htm, (last visited Jan. 22, 2002).

168. Press Release, ACLU, In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Program (July 14, 2000), available at http://www.aclu.org/news/2000/n071400a.html (last visited Jan. 29, 2002).

169. Press Release, EPIC, Lawsuit Seeks Immediate Release of FBI Carnivore Documents (Aug. 2, 2000), available at http://www.epic.org/privacy/carnivore/8_02_release.html (last visited Jan. 29, 2002).

170. Nick Wingfield & Don Clark, *Internet Companies Decry FBI's E-mail Wiretap Plan*, THE WALL STREET JOURNAL, July 12, 2000, at B11A.

technology secretly.[171] This solution satisfied neither the civil libertarians nor the FBI. David Sobel of EPIC said the matter raised "very basic questions of accountability. The suggestion that the use of high-tech law enforcement investigative techniques should result in a departure from our tradition of open judicial proceedings is very troubling."[172] Donald Kerr, assistant director of the FBI's laboratory division, stated that the disclosure of certain information about the KLS would "compromise the use of this technology...and jeopardize the safety of law enforcement personnel."[173]

Secrecy also remains one of the key objections to the use of roving intercepts under FISA. FISA was established in the mid-1970s, after the public was alarmed to learn of the activities of President Nixon and to discover that the NSA had been illegally intercepting telegraph and telephone calls.[174] A congressional committee was created to investigate, and found that nearly every president had authorized warrantless communications surveillance, often for political purposes.[175] Essentially, agencies such as the FBI, CIA, and NSA were able to conduct surveillance without going through normal criminal procedures. The Department of Justice launched its own in-house investigation, resulting in new guidelines for both domestic and foreign intelligence investigations. To prevent future abuses, Congress passed FISA in 1978 to spell out what the NSA (and other intelligence agencies) could and could not do.[176] The NSA had insisted that its activities–especially regarding its methods and technologies–would be severely compromised if discussed in open court. In response, FISA authorized the formation of a special federal court whose proceedings could be completely secret.[177]

---

171. Opinion and Order requiring submission of report "detailing how the key logger device function," United States District Court, District of New Jersey, United States v. Scarfo (August 2001), available at http://www2.epic.org/crypto/scarfo/order_8_7_01.pdf (last visited Jan. 29, 2002).

172. John Schwartz, *US Refuses to Disclose PC Tracking*, NY TIMES, Aug. 25, 2001, at C1.

173. Krim, *supra note 44*.

174. *See* 114 CONG. REC. 14, 750 (1968)

175. *Official report of the Senate Select Committee on Intelligence*, headed by Senator Frank Church, as published in US NEWS AND WORLD REPORT, Dec. 15, 1975, at 61.

176. Jim McGee, *The Rise of the FBI*, WASHINGTON POST MAGAZINE, July 20, 1997, at W10.

177.177. 50 USC 1803.

In short, while the public cannot be informed about all the workings of all the protective technologies, such as Carnivore, because this would impair the usefulness of the technologies, the public can act as the ultimate enforcer of accountability.

C. In conclusion

To determine whether or not a specific public policy measure is legitimate entails more than establishing whether or not it significantly enhances public safety and is minimally intrusive, whether it further undermines already endangered civil rights, or makes it more difficult to deal with public needs. It entails rendering a judgment as to whether or not those who employ any new powers are sufficiently accountable to the various overseers–ultimately the citizenry. Some powers are inappropriate no matter what oversight is provided. However, for those at issue here, the main question is whether there is sufficient accountability. *The remedy, if accountability is found deficient (or excessive), is to adjust accountability and not to deny the measure altogether*. This holds, though, I grant, only if one makes one key assumption examined in the next section.

Whether the specific powers given to the government in regard to the matters at hand are sustaining or undermining the balance between rights and safety depends on how strong each layer of accountability is, whether higher layers enforce lowers ones, and whether there are full complements of layers or not. It is true that there can be too much accountability, such that law enforcement agents would be reluctant to act due to fear that they would be penalized by superiors, by the courts, or by Congress, or be skewered by the press. However, there have been no signs of this since 9/11.

IV. THE ULTIMATE QUESTION

Accountability is ultimately a matter of trust. Plato is said to have raised the issue in asking, who will guard the guardians,[178] or, as it is put in Latin, *quis custodiet ipsos custodes*? Others attribute the question to the Roman satirist Juvenal, who wrote around 2000 years ago.[179] The issue, though, is very much with us. If we do not trust the cops on the beat, we may ask their captains to keep them under closer supervision. If we do not trust the police, we may call on the civil authorities, such as mayors, to scrutinize the police. We may call on the other branches of government–the courts, especially–to serve as checks and balances. However, if we believe that the mayors are corrupt and the judges cannot be trusted either, we have little to fall back on other than the fourth estate. Yet the media, too, is often distrusted.[180]

The question, then, is whom we should distrust and how much. If basically no authority or media figure is trustworthy and "The System" is corrupt, we face a much larger challenge than if, in a few instances, public authorities intercept more e-mail than they are supposed to, or tap some phones they ought not. If someone believes this, she should either move to another country or fight for an entirely new political system.

In contrast, if only some cops, captains, mayors, and other public authorities are corrupt, we have good reason to watch out for such individuals, but not to doubt the political system. We ought, then, to work to improve the various layers of accountability, but also realize that the fact that critics can always come up with some horror stories does not necessarily mean that they are typical of the system.

Although I cannot justify it within the confines of this article, I hold the latter position. Hence, I suggest that one best ignores both claims by public authorities that no strengthening of accountability is needed and the shrillest civil libertarian outcries that sound as if no one is to be trusted. Instead, one is likely to favor reforms that will enhance accountability, rather than

178. Robert O. Keohane, *Governance in a Partially Globalized World*, AMERICAN POLITICAL SCIENCE REVIEW 95, no. 1 (2001), at 1-13.

179. Martin Edmonds, INTERNATIONAL AFFAIRS 62, no. 2 (1986), 290-91 (reviewing MILITARY INTERVENTION IN DEMOCRATIC SOCIETIES, Peter J. Rowe and Christopher J. Whelan, eds.); *Jeffrey Simpson, What Happens when Society's Guardians Need Guardians Themselves?* GLOBE AND MAIL, Sept. 11 1996.

180. SEYMOUR MARTIN LIPSET & WILLIAM SCHNEIDER. THE CONFIDENCE GAP: BUSINESS, LABOR, AND GOVERNMENT IN THE PUBLIC MIND (1987).

denying public authorities the tools they need to do their work (although not necessarily granting them all those they request) in a world in which new technologies have made their service more difficult and in which the threat to public safety has vastly increased.